UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	**No. 3:24-CR-00151**
v.	)	**JUGDE RICHARDSON**
	)	
MATTHEW ISSAC KNOOT	)	

MOTION TO DISMISS COUNTS 1, 4, 5 & 6 OF THE INDICTMENT

The Government claims that Matthew Knoot committed, conspired to commit, or aid-and-abetted the commission of no less than six crimes, including computer fraud, wire fraud, money laundering, aggravated identity theft, and unlawful employment of an unauthorized alien.

The reason? Because (according to the indictment) Knoot, acting at the direction of a person referred to as "Yang Di" (Yang), agreed in exchange for a small fee to install commercially-available remote desktop applications onto a couple of laptops owned by companies that Yang said he worked for so that Yang could log on to the laptops and do his job. Unbeknownst to Knoot, however, Yang evidently used another person's identity to obtain the jobs, meaning that neither he nor the person whose identity he used actually worked for the companies.

Problematically for the Government, however, this theory of criminal liability is untenable. Indeed, even taking all the allegations in the indictment as true, the indictment does not allege a violation of the computer fraud, identity theft, or unlawful-employment-of-an-alien statutes.

Thus, through counsel, and pursuant to Federal Rules of Criminal Procedure 7(c)(1) and 12(b)(3)(B)(v), Knoot moves the Court to dismiss Counts 1, 4, 5, and 6 for failure to state an offense. *United States v. Superior Growers Supply, Inc.*, 982 F.2d 173, 177 (6th Cir. 1992) (affirming dismissal of indictment; reasoning that, "[t]o be legally sufficient, the indictment must assert facts which in law constitute an offense; and which, if proved, would" establish liability).

BACKGROUND

The facts alleged in the indictment, which must be "accept[ed] . . . as true" for purposes of this motion, *see United States v. Reed,* 77 F.3d 139, 140 n.1 (6th Cir. 1996), are as follows:

1. Yang—who is also sometimes referred to in the pleadings as JOHN DOE—is and was (at all times pertinent to the pending charges) "a foreign national residing outside, and not authorized to work in, the United States." (DE 3, Indictment, PageID #5, ¶ 7).

Sometime in or prior to July 2022, someone—the indictment does not say who—stole the identity of a United States citizen named A.M., and, thereafter, Yang used A.M.'s identifying information "to apply for and obtain remote IT work at U.S. companies." (*Id.*).

More specifically:

- On or about July 11, 2022, Yang used A.M.'s name to "obtain[] employment" with Company C as a "senior engineer."
- On or about July 14, 2022, Yang used A.M's name to "obtain[] employment" with Company B as a "mid-level software developer."
- And on or about August 8, 2022, Yang used A.M.'s name to "obtain[] employment" with Company A as a developer.

(*Id.*, PageID #9-10, ¶ 17(a), (b) & (f)).

Yang also apparently secured employment with a fourth company—namely, Company D—but nothing in the indictment suggests that he used A.M.'s identity to get that job. (*Id.*, PageID #6, ¶ 10 (indicating that Yang obtained an employment contract with Company D)).

2. Shortly after Yang secured remote IT work with Companies B and C, he entered into an agreement with Knoot pursuant to which Knoot agreed to "facilitate" Yang's performance of that IT work in exchange for a fee. (*Id.*, PageID #4, ¶ 6; PageID #9, ¶ 17(c)).

In particular, "on or about July 21, 2022" or "July 22, 2022," Knoot agreed: (1) to have laptops issued by "[Yang's] employers" shipped to his residence (2) to "set up[] and host" those

laptops upon receipt, (3) to allow Yang to use his "online business network account and name," and (4) to "assist" Yang with "U.S. employment and tax paperwork." (*Id.*, PageID #10, ¶ 17(c)).

In return, Yang agreed to pay Knoot a "flat rate[] for each hosted laptop," along with a "percentage of" the salary he (Yang) earned performing IT work. (*Id.*, PageID #5-6, ¶ 9).

Between on or about July 25, 2022, and on or about August 10, 2022, Knoot received three laptops—one from Company A, another from Company B, and a third from Company C—and, upon receipt, he used a username and password provided by Yang to logon to those laptops and install a remote desktop application called Anydesk. (*Id.*, PageID #10-11, ¶ 17(e), (h), (k)).

He also received a second laptop from Company B on or about June 22, 2023, and, again, upon receipt, he used a username and password provided by Yang to logon to it and install a remote desktop application called Splashtop Streamer.[1] (*Id.*, PageID #12, ¶ 17(m)).

According to the indictment, "[t]he remote desktop applications" that Knoot installed on the company-issued laptops "enabled [Yang] to work" for those companies from "locations outside the United States, in particular, China, while appearing to the" companies that the work was being performed at Knoot's residence in Nashville, Tennessee. (*Id.*, PageID #5-6, ¶ 9).

3. As Yang completed the IT work the companies assigned to him, the companies paid him a salary—indeed, from July 11, 2022, through August 8, 2023, he earned "approximately $258,553.74" for the work he performed for the companies. (*Id.*, PageID #12, ¶ 17(n)).

And as the paychecks came in, Yang deposited his wages into a bank account maintained at a "U.S. financial institution located in Georgia." (*Id.*, PageID #14, ¶ 21(d)). The account number associated with this deposit account ends in 49277, and, pertinent here, unidentified

[1] The indictment also says that Knoot received a laptop from Company D on or about August 9, 2022, but it does not contain any specific allegations suggesting that Knoot accessed or installed a remote desktop application onto that laptop. (*See id.*, PageID #8, ¶ 16(f) (alleging that Knoot "downloaded . . . remote desktop applications[] onto laptops belonging to . . . Company A, Company B, and Company C," but omitting Company D from the list)).

"[c]onspirators" supposedly opened this account on January 5, 2021—years before Knoot agreed to facilitate Yang's performance of IT work. (*See id.*, PageID #14, ¶ 21(d)).

After Companies A and B transferred Yang's wages into the 49277 account, "[c]onspirators" moved those funds into the Erkomaishvili Account—an account opened in January 2021 through an "Online Payment Platform." (*Id.*, PageID #14, ¶ 21(c)). And between August 21, 2022, and July 3, 2023, unidentified "[c]onspirators" transferred $7,900 from the Erkomaishvili Account into "an account" maintained by Knoot. (*Id.*, PageID #14, ¶ 21(i)).

4. Based on these facts, the Government claims that Knoot committed, conspired to commit, or aided and abetted six federal crimes, including: (1) computer abuse (because he installed remote desktop software onto the company laptops), (2) wire fraud (because Yang lied about his name and location to secure the IT jobs), (3) aggravated identified theft (because "[c]onpirators purchased, stole, or otherwise obtained" A.M.'s identity and Yang used it to secure remote IT work), (4) money laundering (because "[c]onspirators" electronically transferred Yang's wages from one account to another), and (5) unlawful employment of an unauthorized alien.

As explained below, however, the facts alleged (even if proven) simply do not establish the essential elements of Counts 1, 4, 5, and 6. Thus, those counts should be dismissed.

LAW & ARGUMENT

Federal Rule of Criminal Procedure 7(c)(1) provides that an indictment must contain "a plain, concise, and definite written statement of the essential facts constituting the offense[s] charged," and Federal Rule of Criminal Procedure 12(b)(3)(B)(v) states that an indictment is subject to dismissal "without a trial on the merits" if it "fail[s] to state an offense."

Taken together, these rules mean that, "[t]o be legally sufficient," an "indictment must assert facts which in law constitute an offense." *See United States v. Superior Growers Supply,*

Inc., 982 F.2d 173, 177 (6th Cir. 1992); *see also Hamling v. United States*, 418 U.S. 87, 117 (1974) (observing that an indictment must set out the "elements of the offense charged" and that those elements "must be accompanied [by] a statement of the facts and circumstances" giving rise to the "specific offen[se]" charged (quoting *United States v. Hess*, 124 U.S. 483, 487 (1888)).

Or, put another way: An indictment is legally *insufficient* (and is thus ripe for dismissal) if it fails to contain facts which, "if proved, would establish" the elements of the charged crimes. *Superior Growers*, 982 F.3d at 177 (stating that an indictment's factual allegation must be sufficient to "establish prima facie the defendant's commission" of the charged offenses)).

Here, the Government believes that the facts set out in the indictment establish no less than six federal crimes. But a careful review of the elements of those crimes (along with a comparison of those elements to the facts charged in the indictment) reveals otherwise.

A. <u>Counts One & Four: Computer Fraud</u>

The Government claims (in Counts One and Four) that Knoot violated and conspired to violate § 1030(a)(5)(A) of the Computer Fraud & Abuse Act (CFAA) when he installed commercially-available remote desktop applications (namely, Anydesk and Splashtop Streamer) onto laptop computers owned by Companies A, B, and C. The reason? Because by doing so he "enabled" Yang to access those computers. (DE 3, Indictment, PageID #5, 7-12, 16).

Thus, for purposes of this motion, the question is whether those allegations ("if proven") amount to a violation of § 1030(a)(5)(A). *See Superior Growers*, 982 F.3d at 177.

The answer is no. As pertinent here, § 1030(a)(5)(A) of the CFAA criminalizes the act of knowingly transmitting a "program" (or "code" or "command") onto a "protected computer" only if the transmission of the program in question "causes *damage*" to the protected computer. 18 U.S.C. § 1030(a)(5)(A) (emphasis added). And § 1030(e)(8) provides that, for a transmitted

program to "cause[] damage" to a protected computer, the program must "impair[]" the "integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8).

Applying these standards, every court to entertain the issue has held a defendant does not cause to damage to a protected computer—and, therefore, does not violate the CFAA—simply by accessing a computer and then executing on it an action which results in the disclosure of stored information. *Landmark Credit Union v. Doberstein*, 746 F. Supp. 2d 990, 993 (E.D. Wis. 2010) (observing that "[t]here is virtually no support for the proposition that merely accessing and disseminating information from a protected computer" violates "the CFAA"); *see also Motorola, Inc. v. Lemko Corp.,* 609 F. Supp. 2d 760, 769 (N.D. Ill. 2009) (the "CFAA's definition of damage does not cover" harm stemming from "the disclosure [of] confidential information").

Rather, for a transmitted program ("code" or "command") to "cause[] damage," the program must: (1) result in the deletion, corruption, or unavailability of data or information, or (2) cause a computer to run so slowly it no longer functions as intended. *United States v. Nicolescu*, 17 F.4th 706, 715 n.2 (6th Cir. 2021) (finding "damage" when defendant installed a virus onto a computer, which, in turn, "caused infected computers to 'run very slowly'"); *United States v. Soybel*, 13 F.4th 584, 595 (7th Cir. 2021) (finding CFAA "damage" when defendant's actions prevented the victim from using his computer to "servic[e] customers"); *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (finding damage when defendant deleted files), *abrogated on other grounds by Van Buren v. United States*, 593 U.S. 374 (2021).

These outcomes make sense. Congress enacted the CFAA to protect computer data from "virus and worm writers" and to ensure that such data is not intentionally destroyed, altered, or encrypted—not to criminalize conduct which merely causes computer data to be exposed to a third-party. *Citrin*, 440 F.3d at 420 (discussing legislative history); *see also Doberstein*, 746 F.

Supp. 2d at 993 (noting that the CFAA "is not intended to expansively apply to all cases where" confidential information has been shared "by use of a" protected computer).

Here, as described above, the indictment does not include any factual allegations suggesting that Knoot's conduct of installing commercially available remote desktop applications (i.e., Anydesk and Splashtop Streamer) onto the laptops owned by the "victim companies" caused the deletion, corruption, or unavailability of data or information stored on those laptops.

Rather, as explained, it appears the theory underlying the Government's computer fraud claim(s) is that, by installing those applications, Knoot enabled a third-party (Yang) to access the "victim companies'" computer networks. (DE 3, Indictment, PageID #5, ¶ 9).

Because the "[t]here is virtually no support for the proposition that merely accessing" a computer (or information stored on such a computer) amounts to a violation of § 1030(a)(5)(A), *Doberstein*, 746 F. Supp. 2d at 994, the facts the Government alleged in support of its computer fraud claim(s) do not "establish" a "prima facie" violation of the CFAA, *see Superior Growers*, 982 F.3d at 177. Consequently, Counts One and Four of the indictment should be dismissed. *Id.* ("To be legally sufficient, the indictment must assert facts which in law constitute an offense.").

B. <u>Count Five: Aiding & Abetting Aggravated Identity Theft</u>

In Count Five, the Government claims Yang committed aggravated identity theft (when he used A.M.'s identity to secure remote IT work) and that Knoot is criminally responsible for Yang's conduct on an "aiding and abetting" theory. (DE 3, Indictment, PageID #17). To adequately plead the crime of aiding-and-abetting aggravated identity theft, the Government must allege facts showing (among other things): (1) that someone (Yang) committed aggravated identity theft and (2) that the alleged aider-and-abettor (Knoot) did something to help or encourage the commission of that crime with the intent that the crime be committed. *See, e.g.*, Sixth Circuit Pattern Jury

Instruction No. 4.01, *Aiding and Abetting*. And here, the allegations in the indictment (even "if proved") do not establish either element. *See Superior Growers*, 982 F.3d at 177.

1. No one committed aggravated identity theft

To sufficiently plead an aggravated identity theft claim, the Government must charge facts showing that a person, "during and in relation to" the commission of certain specified felonies, "knowingly transfer[red], possesse[d], or use[d], without lawful authority," another person's "means of identification." 18 U.S.C. § 1028A(a)(1) (reciting crime); *see also Dubin v. United States*, 599 U.S. 110, 116 (2023) (discussing and interpreting § 1028A).

Here, the Government's aggravated-identity-theft theory is that Yang "use[d]" A.M.'s identity "during and in relation" to the commission of two felonies—namely, computer and wire fraud—and that he did so "without lawful authority." (DE 3, Indictment, PageID #17). Not so.

a. *Dubin* shows why. The defendant in that case worked for a psychological services company. *Dubin*, 599 U.S. at 114. The "company submitted a claim for reimbursement to Medicaid for psychological testing by a licensed psychologist," but, as it turned out, the employee who performed the services was *not* a licensed psychologist (he was a psychological associate). *Id.* And because the claim for reimbursement overstated the credentials of the service provider, Medicaid reimbursed a greater sum than it would have otherwise. *Id.*

The Government charged the defendant with healthcare fraud (because his misrepresented the credentials of the service provider) and with aggravated identity theft. *Id.* at 115.

Why aggravated identity theft? Because the defendant "included the patient's Medicaid reimbursement number (a 'means of identification')" on the fraudulent reimbursement application. *Id.* In other words, the Government's identity-theft theory was that the defendant "use[d]" the patient's "means of identification" without the patient's authority and that he did so "during and

in relation to" the underlying healthcare fraud—after all, the defendant could *not* have submitted the claim without the patient's Medicaid information. *Id.* at 115 (majority opinion), 137 (Gorsuch, J., concurring) (pointing out that the defendant "could not have successfully billed the insurance provider without accurately offering up some specific patient's name and information").

The district court reluctantly accepted the Government's theory of criminality, and, in a divided opinion, the Fifth Circuit (sitting en banc) affirmed. *Id.* at 115-16 (majority opinion).

The Supreme Court took the case to decide what it means for a person to "*use*[]" (or transfer, possess, etc.) another's "means of identification" "*during and in relation to*" a predicate felony offense. *Id.* at 116-17; 18 U.S.C. § 1028A(a)(1) (emphasis added).

It answered that question as follows: For a person to "use" another's identity "during and in relation" to a predicate felony, the use of the other person's "means of identification" must be "at the *crux* of what makes the predicate offense criminal." *Id.* at 117 (emphasis added), 132. And "[b]eing at the crux of the criminality," the Court explained, "requires" not only a "causal relationship" between the use of the other's identity and the fraud's "success" but *also* that the "means of identification . . . be used in a manner that is fraudulent or deceptive." *Id.*

Justice Gorsuch concurred in the judgment only. He applauded the majority for "reject[ing]" the Government's "unserious position" about the scope of the aggravated-identity-theft statute. *Id.* at 133. But he then went on to explain that, in doing so, the Court may have "stumbled upon a more fundamental problem with § 1028A(a)(1)"—namely, it's unconstitutionally vague. *Id.* As support, Justice Gorsuch posited: "When, exactly, is a 'means of identification' 'at the crux'" of the underlying felony offense? *Id.* at 135. "No doubt[] the answer 'turns on causation, or at least causation often helps to answer the question.'" *Id.* (quoting *United States v. Michael*, 882 F.3d 624, 628 (6th Cir. 2018)). But "how does one even determine

the extent to which a 'means of identification' 'caused' an offense, as compared to the many other necessary inputs?" *Id.* In light of these administrability problems, Justice Gorsuch sympathized: "it is hard not to worry that the Court's 'crux' test will simply become a fig leaf for judges' and jurors' own subject moral judgments about whether . . . the defendant's crime is 'one that warrants a 2-year mandatory minimum'" (which is what § 1028A calls for). *Id.* at 138. And given that "the Constitution's promise of due process means that criminal statutes must provide rules knowable in advance, not intuition discoverable only after a prosecutor has issued an indictment and a judge offers an opinion," Justice Gorsuch concluded that § 1028A(1)(A) was void for vagueness.

b. In light of the above, the question becomes: Assuming the Government has adequately pled computer or wire fraud, has the Government alleged that Yang used A.M.'s identity "during and in relation to" those crimes? Or, in *Dubin*'s terms, was Yang's use of A.M.'s identity at the "crux" of what made the underlying crimes (computer and wire fraud) illegal?

The answer is no. The indictment charges that Yang used A.M.'s identity to obtain remote IT work and to access the victim companies' computers. But nothing in it suggests that he *had* to do so in order to effectuate the alleged scheme or that doing so was the "crux" of what made the under the alleged scheme illegal. *Dubin*, 599 U.S. at 131 (intimating that, for the use of another's identity to be "at the crux of the criminality," the must be at least a "but-for" cause of the underlying crime's 'success'"). This is evident from the fact that Knoot and Yang could've carried out the exact same (alleged) wire and computer fraud scheme without A.M.'s identity. Indeed, if Knoot had secured employment with Companies A, B, C, and D, installed remote software on the laptops, and then sent the laptops to Yang to do the work pursuant to a wage-sharing arrangement, the Government could and would pursue the exact same fraud theories. It could still claim: (1) that Knoot conspired to commit computer fraud when he installed remote desktop applications on

the laptops and allowed Yang to access the companies' network, and (2) that the parties conspired to commit wire fraud when they lied about the name and location of the person completing the assigned IT work. In this way, A.M.'s identity was not the "crux" of what made underlying scheme illegal (assuming, of course, that the alleged scheme was illegal at all). Hence, under *Dubin*, A.M.'s identity was not used "during and in relation to" the predicate felonies.

Not convinced? Consider: The scheme in *Dubin* actually *required* the use of a real patient's identifying information—that is, the defendant there "could not have successfully billed the insurance provider without accurately offering up some specific patient's name and information," *see id.* at 137 (Gorsuch, J., concurring)—yet the majority still held that the use of the patient's means of identification was not the "crux" of what made the scheme criminal, *see id.* at 131-32 (majority opinion). And given that circumstance, if the *Dubin* defendant's conduct did not involve the use of another's identity "during and in relation to" the underlying healthcare fraud, it's hard to see how the use of A.M.'s identity (as alleged) here did.

Still not convinced? Then it appears Justice Gorsuch was right. Section 1028A(a)(1) "is not much better than a Rorschach test. Depending on how you squint your eyes, you can stretch (or shrink) its meaning to convict (or exonerate) just about anyone." *Id.* at 133 (Gorsuch, J., concurring). And that being the case—for the reasons Justice Gorsuch expressed in his *Dubin* concurrence—§ 1028A(a)(1) "simply does too little to specify which individuals deserve the inglorious title of 'aggravated identity thief'" and is therefore void for vagueness. *Id.*

That said, the Government's aggravated-identity-theft theory is a non-starter. A.M.'s identity was not the "crux" of what made the alleged fraud scheme illegal because his identity was unnecessary to the commission of that (alleged) scheme. And if *Dubin*'s "crux" test is satisfied here (but *wasn't* satisfied in *Dubin*, a case where the defendant could not have carried out his

scheme without stealing someone's identity), then there's no principled way to apply the aggravated-identity-theft statute, and, therefore, it's unconstitutionally vague.

2. The indictment does not allege facts showing that Knoot did something to help or encourage the commission of an aggravated identity theft

Further, and setting the above-described problems aside, the charge here is that Knoot aided and abetted aggravated identity theft meaning that, in addition to alleging that an aggravated identity theft was committed, the Government was also required to plead facts showing that Knoot helped or encouraged the commission of that offense "with the intent that the crime be committed." Sixth Circuit Pattern Jury Instruction No. 4.01, *Aiding and Abetting*.

And allegations to that effect are noticeably absent from the indictment. Indeed, the indictment does not even allege facts showing that Knoot knew that A.M.'s identity had been stolen—much less that he intended for Yang to use A.M.'s identity for purposes of deceit.

Accordingly, the aggravated-identity-theft claim must be dismissed. The charge is "legally [in]sufficient" because the indictment does not "assert facts which in law constitution" a violation of § 1028A(1)(A) *See Superior Growers*, 982 F.3d at 177. And even beyond that, as the above efforts to reconcile the charged conduct with *Dubin* prove, § 1028A(1)(A) is void for vagueness.

C. <u>Count Six: Conspiracy to Unlawfully Employ an Unauthorized Alien</u>

Last, the Government claims that Knoot conspired to violate 8 U.S.C. § 1324a(a)(1)(A), a statute which makes it "unlawful for a person or other entity to hire, or to recruit or refer for a fee, for employment in the United States an alien" while "knowing the alien is an unauthorized alien."

Not so. The indictment does not suggest that Knoot "hire[d]" anyone. And for good reason: Knoot is not an "employer." *Chamber of Com. of U.S. v. Whiting*, 563 U.S. 582, 589 (2011) (describing § 1324a as a statute that applies to "employers" and noting that *employers* "that violate" that statute's "strictures may be subjected to both civil and criminal sanctions"). Likewise,

the indictment does not suggest that Knoot "recruit[ed]" or "refer[red]" Yang (or anyone else) for employment. Quite the contrary, the indictment's allegations suggest that Yang had already been hired by Companies B and C *before* Knoot agreed to install remote desktop applications on those companies' computers. (DE 3, PageID #10, ¶¶ 17(a)-(c)). Likewise, nothing in the indictment suggests that Knoot "recruit[ed]" or "refer[red]" Yang for employment with Company A. (*Id.*, PageID #10, ¶17(f)). And finally, as noted above, the indictment says nothing at all about how Yang obtained a job with Company D (nor does it allege that Knoot ever logged on to Company D's laptop or that he installed a remote desktop application on that laptop).

Given these factual deficiencies, and in light of the fact that it appears that 8 U.S.C. § 1324a(a)(1)(A) was only intended to impose liability on W-2 *employers* who hire unauthorized aliens (as opposed to, for instance, persons who allegedly enter into quasi-partnerships with unauthorized aliens), *see Whiting*, 563 U.S. at 589 (noting that "*[e]mloyers* that violate" § 1324a(a)(1)(A) "may be subjected to . . . criminal sanctions"), the indictment does not charge a violation of that statute. As such, the § 1324a(a)(1)(A) claim should be dismissed.

CONCLUSION

In light of the foregoing, Knoot respectfully asks this Court to dismiss Counts 1, 4, 5, and 6 of the indictment for failure to state an offense.

Respectfully submitted,

s/ *David Fletcher*
DAVID FLETCHER
Assistant Federal Public Defender
810 Broadway, Suite 200
Nashville, Tennessee 37203
615-695-6951
David_fletcher@fd.org

Attorney for Matthew Knoot

CERTIFICATE OF SERVICE

I hereby certify that on July 1, 2025 I electronically filed the foregoing *Motion to Dismiss Counts 1,4,5, & 6 of the Indictment* with the U.S. District Court Clerk by using the CM/ECF system, which will send a Notice of Electronic Filing to the following: Joshua Kurtzman, Assistant United States Attorney, 719 Church Street, Suite 3300, Nashville, Tennessee, 37203.

s/ *David Fletcher*
DAVID FLETCHER